UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/730,167	12/05/2003	Thomas A. Crispin	CNTR.2224-C1	2865

23669 7590 03/17/2010

HUFFMAN LAW GROUP, P.C.
1900 MESA AVE.
COLORADO SPRINGS, CO 80906

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
03/17/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO@HUFFMANLAW.NET

Office Action Summary	Application No.	Applicant(s)	
	10/730,167	CRISPIN ET AL.	
	Examiner	Art Unit	
	Thomas Gyorfi	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 February 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22,24,25,27,56-64,66-76 and 79-83* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22,24,25,27,56-64,66-76 and 79-83* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-22, 24, 25, 27, 56-64, 66-76, and 79-83 remain for examination. The amendment filed 2/18/10 amended claims 1 and 56.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/18/10 has been entered.

Response to Arguments

3. Applicant's arguments filed 2/18/10 have been fully considered but they are not persuasive. For the sake of convenience, Examiner reprints herein the most pertinent limitation of claim 1 (for which parallel limitation may be found in claim 56):

> translation logic, configured to translate said atomic cryptographic instruction into associated micro instructions that specify sub-operations required to accomplish said one of the cryptographic operations;
>
> a cryptography unit, configured to receive a first plurality of said associated micro instructions, and configured to execute a plurality of cryptographic rounds on each of said plurality of blocks of input data to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by said control word; and
>
> An x86 integer unit, an x86 floating point unit, an x86 MMX unit, and an x86 SSE unit, wherein said cryptography unit operates in parallel with said x86 integer unit, said x86 floating point unit, said x86 MMX unit, and said x86 SSE unit, to accomplish said one of the cryptographic operations.

At first glance one might be tempted to misconstrue that this limitation implies that each of these additional functional units actually participate in the processing of cryptographic instructions. However, the claim language remains somewhat ambiguous over which units are executing which instructions. As currently written, the claim(s) appear to disclose wherein the cryptographic instruction is broken into a series of microcode instructions, and then the cryptographic microcode is executed by the cryptographic unit while the other recited units work in parallel; support for these limitations appear to be found at paragraph 0050 on pages 31-33 of the instant specification. From Applicant's remarks Examiner surmises that it is Applicant's contention that when a cryptographic instruction of the instant invention is translated into microcode, some portion of the results are cryptographic microcode, some other portion are MMX microcode, yet another portion as SSE microcode, etc. However, the specification does not actually support this interpretation; it does not follow from any explicit disclosure in the specification as to how what is produced by the translation logic should be connected to each of the various functional units. It should also be noted that each of the functional units of the instant microprocessor are strictly limited in the types of operations they may perform: the cryptographic unit only performs cryptographic work; the MMX unit, MMX instructions, etc.; one of ordinary skill in the art would have no reason to expect e.g. an MMX unit to execute cryptographic microcode that would befit the cryptographic unit, for example. Furthermore, even assuming *arguendo* that it were clear that the translation logic produced microcode intended for execution on each of those units, the claims only recite that a "first plurality" of microcode is executed by

the cryptographic unit, but there is no corresponding "second plurality" or the like that would correspond to micro-instructions intended for execution by any of the remaining units; accordingly, one could construe the claim term "first plurality of said associated micro instructions" to represent the entirety of the micro-instructions produced by the translation step. In that case, Kessler as previously cited discloses wherein a cryptographic instruction can be broken down into a series of micro-instructions, all of which are intended to be executed solely by a cryptographic unit. Accordingly, the claims encompass at least this embodiment, and in said embodiment the work of the MMX unit, SSE unit, etc. are clearly seen to be extra-solution activity that does not materially affect the ability of a cryptographic unit to perform cryptographic work. It is further noted that, while Examiner and Applicant agree that the Best reference predates the invention of several of the aforementioned units, Applicant's arguments against Best are moot as it is simply enough that the conventional microprocessor actually have the recited functional units in order to satisfy the claim language, for the reasons discussed *supra*. Examiner also respectfully submits that it would be absurd to expect one of ordinary skill in the art attempting to implement the Best invention to necessarily limit oneself to the use of e.g. an 8086 processor that would have been a contemporary microprocessor at the time of the Best invention, particularly as those early generation x86 processors had long since been removed from the market and were generally no longer available.

Claim Rejections - 35 USC § 103

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1-6, 11, 12, 24, 25, 27, 56-60, 66, and 79-83 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler et al. (U.S. Patent 6,789,147) in view of Bakhle et al. (U.S. Patent 6,021,201) in view of Best (U.S. Patent 4,278,837) in view of "PC Hardware in a Nutshell" (originally supplied in the Office Action mailed 5/13/09; hereinafter, "Thompson").

Regarding claim 1:

Kessler discloses a processor apparatus for performing a cryptographic operation, the apparatus comprising: fetch logic, configured to fetch an instruction flow from memory for execution by a processor (col. 4, line 59 – col. 5, line 36), said instruction flow comprising an instruction, configured to direct said processor to perform the cryptographic operation (col. 4, lines 10-16; col. 5, lines 29-36; Figure 7), wherein said cryptographic instruction prescribes one of the cryptographic operations (Figure 3); said cryptographic operation comprising: an opcode field, configured to prescribe that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory (element 302 of Fig. 3; col. 5, lines 37-50); and a repeat prefix field, coupled to said opcode field, configured to indicate that the cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a plurality of blocks of input data (element 310 of Fig.3; col. 5, line 50 – col. 6, line 10);

and a cryptography unit, disposed within execution logic in said processor, configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by said control word (col. 9, lines 7-55); and an integer unit, disposed within execution logic in said processor and coupled in parallel with said cryptography unit, configured to execute a plurality of integer operations that are required to accomplish the cryptographic operation (col. 9, lines 15-20).

Kessler does not explicitly disclose wherein the cryptographic instructions to be executed are atomic in nature. However, Bahkle discloses a related cryptographic coprocessor that implemented this limitation (col. 5, lines 15-25). It would have been obvious to one of ordinary skill in the art to ensure the atomic operation of the cryptographic instructions executed by the Kesller processor; one would have been motivated to do so because it prevents the various functional units within said processor from overwriting shared memory buffers and thus corrupting the results produced by other operations being performed within said processor (col. 12, lines 15-30).

The processor disclosed by Kessler is a coprocessor, which by itself does not conform to Applicant's preferred definition of "microprocessor" established in the specification. However, Best discloses wherein microprocessors with dedicated cryptographic functionality could be employed in an apparatus, wherein said microprocessor is a hybrid consisting of a conventional microprocessor and a cryptographic coprocessor combined into one single, indivisible microprocessor that behaves in exactly the manner as the "microprocessor" of the instant application (col.

19, lines 20-60; Figures 17 & 18). Additionally, Best clearly discloses wherein the microprocessor has a fetch unit disposed within itself configured to fetch an application program from memory by said microprocessor (e.g. col. 6, lines 15-20). The claims are thus obvious because the substitution of Kessler's cryptographic coprocessor in lieu of the default cryptographic coprocessor already disclosed by Best for use as the cryptographic unit of Best's hybrid microprocessor would have yielded predictable results to one of ordinary skill in the art by the time of the instant invention.

Best places no limitations as to the specific architecture employed by the prior art microprocessor functional unit of the hybrid microprocessor; nevertheless, Thompson discloses wherein Intel x86 microprocessors had by the time of the instant invention become the dominant variety of microprocessor in the general marketplace (Thompson, page 8, "4.2 Intel Processors", and furthermore by the time of the instant invention a contemporary x86 processor would comprise an x86 integer unit, x86 floating point unit, x86 MMX unit, and x86 SSE unit (see the discussion of the Pentium IV on pages 24-28) It would have been obvious to one of ordinary skill in the art to substitute e.g. a Pentium IV microprocessor in lieu of the generic microprocessor of Best (when combined with Kessler and Bahkle as discussed *supra*) resulting in a hybrid microprocessor comprising these functional units operating in parallel with the cryptographic unit, as the substitution of one known element for another would have yielded predictable results to one of ordinary skill in the art at the time of the instant invention.

Regarding claim 56:

Kessler discloses an apparatus for performing cryptographic operations, comprising: fetch logic, disposed within a processor, configured to fetch an instruction flow from memory for execution by a processor by said processor (col. 4, line 59 – col. 5, line 36), said instruction flow comprising an instruction, configured to direct said processor to perform the cryptographic operation (col. 4, lines 10-16; col. 5, lines 29-36; Figure 7), wherein said cryptographic instruction prescribes one of the cryptographic operations (Figure 3); said cryptographic operation comprising: an opcode field, configured to prescribe that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory (element 302 of Fig. 3; col. 5, lines 37-50); and a repeat prefix field, coupled to said opcode field, configured to indicate that the cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a plurality of blocks of input data (element 310 of Fig.3; col. 5, line 50 – col. 6, line 10); translation logic, disposed within said processor, configured to translate said cryptographic instructions into associated micro instructions that specify sub operations required to accomplish said one of the cryptographic operation (e.g. col. 8, lines 11-16); and a cryptography unit, disposed within execution logic in said processor, configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by said control word (col. 9, lines 7-55).

Kessler does not explicitly disclose wherein the cryptographic instructions to be executed are atomic in nature. However, Bahkle discloses a related cryptographic coprocessor that implemented this limitation (col. 5, lines 15-25). It would have been obvious to one of ordinary skill in the art to ensure the atomic operation of the cryptographic instructions executed by the Kesller processor; one would have been motivated to do so because it prevents the various functional units within said processor from overwriting shared memory buffers and thus corrupting the results produced by other operations being performed within said processor (col. 12, lines 15-30).

The processor disclosed by Kessler is a coprocessor, which by itself does not conform to Applicant's preferred definition of "microprocessor" established in the specification. However, Best discloses wherein microprocessors with dedicated cryptographic functionality could be employed in an apparatus, wherein said microprocessor is a hybrid consisting of a conventional microprocessor and a cryptographic coprocessor combined into one single, indivisible microprocessor that behaves in exactly the manner as the "microprocessor" of the instant application (col. 19, lines 20-60; Figures 17 & 18). Additionally, Best clearly discloses wherein the microprocessor has a fetch unit disposed within itself configured to fetch an application program from memory by said microprocessor (e.g. col. 6, lines 15-20). The claims are thus obvious because the substitution of Kessler's cryptographic coprocessor in lieu of the default cryptographic coprocessor already disclosed by Best for use as the cryptographic unit of Best's hybrid microprocessor would have yielded predictable results to one of ordinary skill in the art by the time of the instant invention.

Best places no limitations as to the specific architecture employed by the prior art microprocessor functional unit of the hybrid microprocessor; nevertheless, Thompson discloses wherein Intel x86 microprocessors had by the time of the instant invention become the dominant variety of microprocessor in the general marketplace (Thompson, page 8, "4.2 Intel Processors", and furthermore by the time of the instant invention a contemporary x86 processor would comprise an x86 integer unit, x86 floating point unit, x86 MMX unit, and x86 SSE unit (see the discussion of the Pentium IV on pages 24-28) It would have been obvious to one of ordinary skill in the art to substitute e.g. a Pentium IV microprocessor in lieu of the generic microprocessor of Best (when combined with Kessler and Bahkle as discussed *supra*) resulting in a hybrid microprocessor comprising these functional units operating in parallel with the cryptographic unit, as the substitution of one known element for another would have yielded predictable results to one of ordinary skill in the art at the time of the instant invention.

Regarding claims 2 and 83:

Kessler further discloses wherein the cryptographic operations are accomplished at the level of system privileges afforded to application programs (SSL being a component of web browser applications: col. 4, lines 5-10).

Regarding claims 3 and 57:

Kessler further discloses an encryption operation encrypting a plurality of blocks of input data to generate a plurality of ciphertext blocks (e.g. col. 2, lines 13-14 etc.)

Regarding claims 4 and 58:

Kessler further discloses an decryption operation decrypting a plurality of blocks of input data to generate a plurality of plaintext blocks (Ibid).

Regarding claims 5 and 59:

Kessler further discloses using AES (col. 9, lines 13-15; Figure 8, element 807).

Regarding claims 6 and 60:

Kessler further discloses a block cipher mode to be employed in accomplishing the cryptographic operations (inherent to the block ciphers taught in col. 9, lines 10-20).

Regarding claim 11:

Kessler further discloses wherein the atomic instruction proscribes that the cryptographic operations be accomplished on a plurality of text blocks (Figure 7)

Regarding claims 12 and 66:

It is now taken as an admission of prior art that the "prior art microprocessor" component of the hybrid microprocessor disclosed by Best would be an x86 processor, with instructions prescribed in the x86 instruction format; even were that not so, it should be logically self-evident that an x86 compatible processor employed as the prior art microprocessor of Best could inherently process x86 instructions.

Regarding claims 24 and 79:

Kessler further discloses block cipher logic, configured to perform a plurality of cryptographic rounds on each of said plurality of blocks of input data according to said one of the block cryptographic operations to produce said corresponding plurality of output text blocks (col. 9, lines 7-44); and key RAM, operatively coupled to said block cipher logic, configured to store a key schedule, said key schedule comprising a plurality of round keys, each corresponding to a plurality of cryptographic rounds, and configured to provide each of said plurality of round keys to said block cipher logic for performance of said each of said plurality of cryptographic rounds (col. 9, lines 23-55).

Regarding claims 25 and 80:

Kessler further discloses wherein said block cipher logic id divided into two or more stages, whereby said plurality of cryptographic rounds are simultaneously performed on two or more of said plurality of blocks of data (inherent to at least the AES and 3DES algorithms disclosed on col. 9, lines 10-20).

Regarding claims 27 and 82:

Kessler further discloses wherein said opcode field directs said cryptography unit to load one of said each of said plurality of input text blocks and to perform said plurality of cryptographic rounds (col. 5, lines 40-50).

Regarding claim 81:

Kessler further discloses an integer unit, coupled in parallel with said cryptography unit, configured to execute a plurality of integer operations that are required to accomplish the cryptographic operations (arithmetic unit: col. 9, lines 15-20).

6. Claims 7-10 and 61-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler in view of Bakhle in view of Best in view of Thompson as applied to claims 6 and 60 above, and further in view of the "Applied Cryptography, 2nd Edition" (hereinafter, "Schneier").

Regarding claims 7-10 and 61-64:

Although Kessler and Best both disclose using block cipher modes for at least some of the supported encryption algorithms, they do not explicitly mention any of the modes listed in these claims. However, Schneier teaches that each mode (ECB, CBC, CFB, and OFB) were well known in the art (pages 193-206); accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use any of these modes in the cryptographic processor disclosed by Kessler, let alone the hybrid of Best modified by Kessler; each mode has its own particular advantages as disclosed by Schneier (page 209, as appropriate).

7. Claims 13-22 and 67-76 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler in view of Bakhle in view of Best in view of Thompson as applied to claims 1 and 56 above, and further in view of Johns-Vano et al. (U.S. Patent 6,026,490).

Regarding claims 13 and 67:

Although Kessler and Best both disclose at least one register (Kessler: element 220 of Figure 2; Best: col. 5, lines 35-50 and Figures 8 & 9), it is unclear as to whether the instruction implicitly references a plurality of registers in the device. However, Johns-Vano discloses that the instruction set of a cryptographic processor implicitly references a plurality of internal registers (elements 558, 560, 564, 552, 566, and 556 of Figure 1). It would have been obvious to one of ordinary skill in the art at the time the invention was made for a cryptographic processor to employ a plurality of registers. One would do so because using hardware registers would be conducive to making a cryptographic processing engine suitable for manufacture in semiconductor foundries thereby reducing manufacturing costs (col. 2, lines 28-33). It is also noted that x86 processors were already known to have registers (e.g. Wikipedia, pages 2-3).

Regarding claims 14 and 68:

Johns-Vano further discloses a first register, wherein contents of said first register comprise a pointer to a first memory address, said first memory address

specifying a first location in said memory for access of a plurality of input text blocks upon which the cryptographic operations is to be accomplished (col. 5, lines 1-55).

Regarding claims 15 and 69:

Johns-Vano further discloses a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing the cryptographic operations upon a plurality of input text blocks (col. 5, lines 1-55).

Regarding claims 16 and 70:

Johns-Vano further discloses a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks (col. 5, lines 1-55).

Regarding claims 17 and 71:

Johns-Vano further discloses a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in said memory for access to cryptographic key data for use in accomplishing the cryptographic operations (col. 5, lines 1-55).

Regarding claims 18 and 72:

Kessler and Johns-Vano further disclose wherein said cryptographic key data comprises a cryptographic key (Kessler: col. 6, lines 40-50; Johns-Vano: col. 7: 1-5).

Regarding claims 19 and 73:

Kessler further discloses wherein said cryptographic key data comprises a cryptographic key schedule (inherent to the algorithms used in col. 9, lines 10-20).

Regarding claims 20 and 74:

Johns-Vano further discloses a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in said memory for access of an initialization vector for use in accomplishing the cryptographic operations (col. 5, lines 1-55).

Regarding claims 21 and 75:

Johns-Vano further discloses a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in said memory for access of said control word for use in accomplishing the cryptographic operations, wherein said control word prescribes cryptographic parameters for cryptographic operations (col. 5, lines 1-55).

Regarding claims 22 and 76:

Kessler further discloses an encryption/decryption field, configured to prescribe whether the cryptographic operation is an encryption operation or a decryption operation (col. 5, lines 50-60).

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
3/10/10

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435